



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/663,863	09/15/2000	Ilya Minkin	NA11P007/00.045.01	4199

28875 7590 03/05/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP  
P.O. BOX 721120  
SAN JOSE, CA 95172-1120

EXAMINER

TRAN, TONGOC

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 03/05/2004

6

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/663,863

Applicant(s)

MINKIN ET AL.

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 15 September 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 5.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. This office action is in response to applicants' application serial no. 09/663,863 filed on 9/15/2000.

#### ***Information Disclosure Statement***

2. The information disclosure statement (IDS) submitted on 8/5/2002 has been considered by the examiner.

#### ***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 24-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Wiegel (U.S. Patent No. 6,484,261).

In respect to claim 24, a method for establishing network security, comprising the steps of:

(a) providing a plurality of network objects of a network and a plurality of rule sets; (b) associating the network objects with the rule sets; (c) when the rule sets

Art Unit: 2134

include a plurality of policy rules that govern actions relating to the identified network objects during operation of the network (see col. 1, lines 44-61 and 8, lines 12-26).

In respect to claim 25, Wiegel discloses the method as recited in claim 24, wherein a user is allowed to associate the network objects with the rule sets via a graphical user interface (see col. 1, lines 10-15).

In respect to claim 26, Wiegel discloses the method as recited in claim 24, wherein each policy rule of the reconciled rule sets includes a rule action selected from the group consisting of:

permitting an action relating to the identified network objects, denying an action relating to the identified network objects, and conditionally denying an action relating to the identified network objects (see, col. 1, lines 1-15).

In respect to claim 27, Wiegel discloses the method as recited in claim 26, wherein an action relating to the identified network objects is permitted if no policy rules deny the action, at least one policy rule conditionally denies the action, and at least one policy rule permits the action (see col. 18, lines 1-40).

In respect to claim 28, Wiegel discloses the method as recited in claim 24, wherein an action relating to the identified network objects is denied if none of the policy rules permit the action (see col. 9, lines 25-30).

In respect to claims 29-33, the claim limitations are computer program product claims that are substantially similar to method claims 24-28. Therefore, claims 29-33 are rejected based on the similar rationale.

Art Unit: 2134

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-6, 10-17 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel (U.S. Patent No. 6,484,261) in view of Bal et al. (U.S. Patent No. 6,691,168, hereinafter Bal).

In respect to claim 1, Wiegel discloses a method for providing network security features, comprising the steps of:

(a) identifying a plurality of network objects, (b) retrieving rule sets-associated with at least one of the identified network objects, the rule sets including a plurality of policy rules that govern actions relating to the identified network objects (see Wiegel, col. 8, lines 12-26);

Wiegel does not disclose but Bal discloses:

(c) reconciling overlapping policy rules of the rule sets amongst the network objects; and (d) executing the reconciled rule sets (see col. 11, lines 15-30 and 45-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Wiegel's network security policy management with the teaching of Bal's method of high speed network rule processing that use different search strategies to handle different situations between disjoint (no overlapped

rules) and non-disjoint (overlapped rules) set of rules in order to speed up the search (see col. 11, lines 18-29).

In respect to claim 2, Wiegel and Bal disclose the method as recited in claim 1, wherein each policy rule of the reconciled rule sets includes a rule action selected from the group consisting of permitting an action relating to the identified network objects, denying an action relating to the identified network objects, and conditionally denying an action relating to the identified network objects (see Wiegel, col. 10, lines 1-15).

In respect to claim 3, Wiegel and Bal disclose the method as recited in claim 2, wherein an action relating to the identified network objects is permitted if no policy rules deny the action, at least one policy rule conditionally denies the action, and at least one policy rule permits the action (see Wiegel, col. 18, lines 1-40).

In respect to claim 4, Wiegel and Bal disclose the method as recited in claim 2, wherein the policy rules denying the action are evaluated first, the policy rules conditionally denying the action are evaluated second, and the policy rules permitting the action are evaluated third (see Wiegel, col. 9, lines 25-34 and col. 18, lines 1-40).

In respect to claim 5, Wiegel and Bal disclose the method as recited in claim 1, wherein an action relating to the identified network objects is denied if none of the policy rules permit the action (see Wiegel, col. 9, lines 25-30).

In respect to claim 6, Wiegel and Bal disclose the method as recited in claim 1, wherein an action relating to the identified network objects is denied if none of the policy rules match a request for the action (see Wiegel, col. 9, lines 26-30).

In respect to claim 10, Wiegel and Bal disclose the method as recited in claim 1., wherein the rule sets are associated with a particular network object (see Wiegel, col. 8, lines 12-26).

In respect to claim 11, Weigel and Bal disclose the method as recited in claim 1, wherein a protocol configuration enforced by a related proxy is selected from a hierarchal list if an action is permitted by more than one rule (see col. 3, line 59-col. 4, line 6 and col. 10, lines 1-15).

In respect to claims 12-17 and 21-22, the claim limitations are computer program product claims that are substantially similar to method claims 1-6 and 10-11. Therefore, claims 12-17 and 21-22 are rejected based on the similar rationale.

In respect to claim 23, the claim limitation is a system claim that is substantially similar to method claim 1. Therefore, claim 23 is rejected based on the similar rationale.

5. Claims 7-9 and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel (U.S. Patent No. 6,484,261) in view of Bal et al. (U.S. Patent No. 6,691,168, hereinafter Bal) and further in view of Engel et al. (U.S. Patent No. 6,519,636).

In respect to claims 7-9, Wiegel and Bal disclose the method as recited in claim 1. Wiegel and Bal do not disclose wherein executing the reconciled rule sets includes combining the rule sets into a single rule set; removing duplicate policy rules of the rule sets and notifying a user of conflicting policy rules of the rule sets.

However, Engel discloses rules are modified when duplicate rules is found and need to be changed (see col. 13, lines 5-19). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Wiegel and Bal's rule-based network management method with the teaching of Engel's by merging or removing overlapping rules to eliminate redundant rules in the database.

In respect to claims 18-20, the claim limitations are computer program product claims that are substantially similar to method claims 7-9. Therefore, claims 18-20 are rejected based on the similar rationale.

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Coss discloses a method and apparatus for a computer network firewall with dynamic rule processing with the ability to dynamically alter the operations of rules.

-Nakazawa discloses a network system using a firewall dynamic control method.

-Reid et al. Discloses a system and method for controlling interactions between networks.

-Flint et al. Discloses a system and method for implementing a security policy.

-Coss et al. Disclose a methods and apparatus for a computer network firewall with cache query processing.

-Zenchelsky et al. Disclose a session cache and rule caching method for a dynamic filter.

Art Unit: 2134

-Putzolu discloses a policy-based network management system using dynamic policy generation.

-Nessett et al. Disclose a multilayer firewall system.

-Wood et al. disclose a security architecture with environment sensitive credential sufficiency evaluation.

-Plutowski discloses a system for combining plurality of input control policies to provide a compositional output control policy.

-Stockwell et al. disclose generalized security policy management system and method.

-Coss et al. Disclose a method and apparatus for a computer network firewall with proxy reflection.

-Kloth discloses rule based IP data processing.

--Durham et al. Discloses a system and method for managing actions provided by a network using a policy tree.

Ahlstrom et al. Disclose recognizing and processing conflicts in network management policies.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone

Art Unit: 2134

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran  
Art Unit: 2134

TT

March 2, 2004

*Matthew B. Smithers*  
MATTHEW SMITHERS  
PRIMARY EXAMINER  
*Art Unit 2137*